enisa

EUROPEISKA UNIONENS
CYBERSÄKERHETSBYRÅ

Cybersäkerhetsvägledning för små och medelstora företag

12 STEG

FÖR ATT SKYDDA DIN VERKSAMHET

Under covid-19-krisen framgick det tydligt vilken stor betydelse internet och datorer har för små och medelstora företag. För att kunna driva sin verksamhet under pandemin blev många små och medelstora företag tvungna att vidta kontinuitetsåtgärder, bland annat börja använda molntjänster, förbättra sina internettjänster, uppgradera sina webbplatser och möjliggöra för personalen att distansarbeta.

I den här broschyren lyfter vi fram tolv övergripande steg som små och medelstora företag kan vidta för att trygga sina system och sin verksamhet. Den kompletterar den mer detaljerade Enisa-rapporten ***Cybersecurity for SMES – Challenges and Recommendations***.

1 SKAPA EN BRA CYBERSÄKERHETS KULTUR

TILLDELA LEDNINGSANSVAR

En god cybersäkerhet är avgörande för små och medelstora företags fortsatta framgångar. Ansvaret för denna kritiska funktion bör tilldelas en person i organisationen som kan säkerställa att lämpliga resurser i form av mantimmar avsätts för cybersäkerhet, att programvara, tjänster och maskinvara för cybersäkerhet köps in, att personalen får utbildning i ämnet och att effektiva cybersäkerhetspolicyer utarbetas.

VINN MEDARBETARNAS ENGAGEMANG

Vinn medarbetarnas engagemang genom effektiv kommunikation om cybersäkerhet från ledningen, ledningens öppna stöd för cybersäkerhetsinitiativ, lämplig utbildning till medarbetarna samt tydliga och specifika regler för medarbetarna samlade i cybersäkerhetspolicyer.

PUBLICERA CYBERSÄKERHETSPOLICYER

Företaget ska ha cybersäkerhetspolicyer med tydliga och specifika regler som anger hur medarbetarna förväntas uppföra sig när de använder företagets miljö, utrustning och tjänster avseende IKT. Dessa policyer ska också tydliggöra konsekvenserna om en medarbetare inte efterlever policyerna. Policyerna ska revideras och uppdateras regelbundet.

GENOMFÖR CYBERSÄKERHETSREVISIONER

Regelbundna revisioner bör genomföras av personer med lämplig kunskap, kompetens och erfarenhet. Revisorerna ska vara oberoende, och det kan vara antingen en utomstående entreprenör eller en internrevisor på företaget som är oberoende av den dagliga it-driften.

GLÖM INTE DATASKYDD

Enligt EU:s allmänna dataskyddsförordning[1] ska alla små och medelstora företag som behandlar eller lagrar personuppgifter som tillhör personer med hemvist i EU/EES säkerställa att lämpliga säkerhetskontroller finns på plats för att skydda sådana uppgifter. Detta inkluderar att säkerställa att eventuella tredje parter som arbetar för företagets räkning har lämpliga säkerhetsåtgärder på plats.

1 Den allmänna dataskyddsförordningen https://ec.europa.eu/info/law/law-topic/data-protection_en

2

TILLHANDAH ÅLL LÄMPLIG UTBILDNING

Tillhandahåll alla medarbetare regelbunden utbildning i cybersäkerhetsmedvetenhet för att säkerställa att de känner igen och kan hantera de olika cybersäkerhetshoten. Dessa utbildningar bör skräddarsys efter företaget och fokusera på verkliga situationer.

Tillhandahåll särskild cybersäkerhetsutbildning till de som är ansvariga för hanteringen av cybersäkerhet inom företaget för att säkerställa att de har den kunskap och kompetens som krävs för jobbet.

3

SÄKERSTÄLL EFFEKTIV HANTERING AV TREDJE PART

Säkerställ att alla leverantörer, i synnerhet de som har åtkomst till känsliga uppgifter och/eller system, hanteras aktivt och uppfyller överenskomna säkerhetsnivåer. Det ska finnas avtal som reglerar hur leverantörerna ska uppfylla säkerhetskraven.

4

UTVECKLA EN INCIDENTRESPONSPLAN

Utarbeta en formell incidentresponsplan som innehåller tydliga riktlinjer, roller och ansvarsområden som säkerställer att alla säkerhetsincidenter hanteras i rätt tid och på ett professionellt och korrekt sätt. För att snabbt kunna reagera på säkerhetshot är ett förslag att undersöka vilka verktyg som finns för att övervaka och skapa varningar när misstänkt aktivitet eller säkerhetsöverträdelser inträffar.

5 SÄKERSTÄLL SYSTEMÅTKOMST

Uppmuntra alla att använda en lösenfras, en grupp av minst tre slumpmässiga, vanliga ord kombinerade till en fras som är både säker och lätt att komma ihåg. Tänk på följande om du väljer ett typiskt lösenord:

- Se till att det är långt, består av små och stora bokstäver, eventuellt även siffror och specialtecken.
- Undvik uppenbara val av lösenord, t.ex. ”lösenord”, sekvenser av bokstäver eller siffror, t.ex. ”abc” eller ”123”.
- Undvik att använda personlig information som går att hitta på internet.

Oavsett om du använder lösenfraser eller lösenord ska du tänka på följande:

- Återanvänd dem inte på andra platser.
- Dela dem inte med kollegor.
- Aktivera multifaktorsautentisering.
- Använd en lösenordshanterare.

6 SÄKRA ENHETER

Ett avgörande steg i cybersäkerhetsprogrammet är att hålla de enheter som medarbetarna använder säkra, oavsett om det är stationära eller bärbara datorer, surfplattor eller smarttelefoner.

SE TILL ATT INSTALLERA PATCHAR OCH UPPDATERINGAR AV PROGRAMVARAN

Använd helst en central plattform för patchhantering. Små och medelstora företag bör

- regelbundet uppdatera all sin programvara,
- alltid aktivera automatiska uppdateringar när det är möjligt,
- identifiera programvara och maskinvara som kräver manuell uppdatering,
- även räkna med mobila enheter och enheter för sakernas internet.

VIRUSSKYDD

En centralt hanterad virusskyddslösning bör implementeras på alla enheter och hållas uppdaterad för att säkerställa fortsatt effektivitet. Installera inte piratkopierade program, eftersom de kan innehålla sabotageprogram.

ANVÄND VERKTYG SOM SKYDDAR E-POST OCH WEBB

Använd lösningar som blockerar skräppost och e-post med länkar till osäkra webbplatser, skadliga bilagor, som kan innehålla virus, och nätfiske.

KRYPTERING

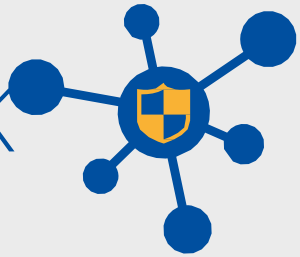
Skydda data genom kryptering. Små och medelstora företag bör säkerställa att data i mobila enheter, däribland bärbara datorer, smarttelefoner och surfplattor, är krypterade. Se till att data som överförs via offentliga nätverk, t.ex. wifi-nätverk på hotell eller flygplatser, krypteras, antingen med hjälp av ett VPN (virtuellt privat nätverk) eller genom att använda en säker anslutning via ett SSL/TLS-protokoll för åtkomst till webbplatser. Säkerställ att de egna webbplatserna använder lämplig krypteringsteknik för att skydda klientdata som färdas genom internet.

IMPLEMENTERA HANTERING AV MOBILA ENHETER

För att underlätta distansarbete tillåter många små och medelstora företag medarbetarna att använda sina egna bärbara datorer, surfplattor och/eller smarttelefoner. Det medför allvarliga säkerhetsproblem när det gäller känsliga företagsdata som finns lagrade i dessa enheter. Ett sätt att hantera risken är att använda en MDM-lösning (Mobile Device Management), vilket gör att företaget kan

- kontrollera vilka enheter som har behörighet till företagets system och tjänster,
- säkerställa att enheten har ett uppdaterat virusprogram installerat,
- avgöra om enheten är krypterad,
- bekräfta att enheten har uppdaterade patchar installerade,
- se till att enheten är skyddad av en pinkod och/eller ett lösenord,
- rensa alla företagsdata från enheten på distans om ägaren till enheten skulle rapportera att den försvunnit eller blivit stulen, eller om ägarens anställning i företaget skulle upphöra.

7 SÄKRA NÄTVERKET



ANVÄND BRANDVÄGGAR

Brandväggar hanterar all trafik in och ut från nätverket och är ett kritiskt verktyg för att skydda företagets system. Brandväggar bör användas för att skydda alla kritiska system, i synnerhet för att skydda företagets nätverk från internet.

SE ÖVER LÖSNINGAR FÖR FJÄRRÅTKOMST

Små och medelstora företag bör regelbundet se över sina verktyg för fjärråtkomst för att säkerställa att de är säkra, i synnerhet

- säkerställa att alla patchar och uppdateringar i programvara för fjärråtkomst körs,
- begränsa fjärråtkomst från misstänkta geografiska platser eller vissa IP-adresser,
- begränsa medarbetarnas fjärråtkomst till de system och datorer som de behöver för sitt arbete,
- kräva starka lösenord för fjärråtkomst och där så är möjligt aktivera multifaktorsautentisering,
- säkerställa att övervakning och larm är aktiverat som varnar för misstänkta attacker eller ovanlig misstänkt aktivitet.

8 FÖRBÄTTRA DEN FYSISKA SÄKERHETEN

Lämpliga fysiska kontroller bör användas varhelst det finns viktig information. Ett företags bärbara dator eller en smarttelefon får exempelvis inte lämnas oövervakad i baksätet på en bil. Varje gång en användare lämnar sin dator bör den låsas. Alternativt kan en autolåsfunktion aktiveras på enheter som används för affärssyften. Känsliga utskrifter får heller inte lämnas utan uppsikt och ska när de inte används låsas in.

9 SÄKERHETSKOPIERA

För att möjliggöra återställning av viktig information ska det finnas säkerhetskopior, eftersom det är ett effektivt sätt att återhämta sig från katastrofer såsom angrepp med utpressningsprogram. Nedanstående regler bör följas när det gäller säkerhetskopiering:

- Säkerhetskopiering ska ske regelbundet och automatiskt när så är möjligt.
- Säkerhetskopior ska förvaras separat från företagets produktionsmiljö.
- Säkerhetskopior ska krypteras, i synnerhet om de flyttas mellan olika platser.
- Möjligheten att regelbundet återställa data från säkerhetskopiorna ska testas. Helst ska man regelbundet testa att göra en fullständig återställning från början till slut.

10 MOLNTJÄNSTER

Molnbaserade lösningar erbjuder många fördelar, men innefattar även en del unika risker, vilket små och medelstora företag bör överväga innan de väljer en molnleverantör. Enisa har publicerat vägledningen *Cloud Security Guide for SMEs*[2], som små och medelstora företag bör läsa innan de migrerar till molnet.

När företaget väljer molnleverantör bör man säkerställa att inga lagar eller förordningar överträds vad gäller lagring av data, i synnerhet personuppgifter, utanför EU/EES. I EU:s dataskyddsförordning krävs exempelvis att personuppgifter som tillhör personer med hemvist i EU/EES inte lagras eller överförs utanför EU/EES om inte särskilda villkor är uppfyllda.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 SÄKRA WEBBPLATSER

Små och medelstora företag måste säkerställa att deras webbplatser är konfigurerade och underhålls på ett säkert sätt och att alla personuppgifter och finansiella data, t.ex. kreditkortsuppgifter, är skyddade på lämpligt sätt. Detta innefattar regelbundna säkerhetstester av webbplatser för att identifiera potentiella svagheter i säkerheten och regelbundna revisioner för att säkerställa korrekt underhåll och uppdatering av webbplatser.

12 SÖKA OCH DELA INFORMATION

Ett effektivt verktyg i kampen mot it-brottslighet är informationsdelning. Informationsdelning gällande it-brottslighet är avgörande för att små och medelstora företag ska få en bättre förståelse för de risker de står inför. Det är mer sannolikt att ett företag vidtar åtgärder för att säkra sina system om det hör talas om cybersäkerhetsutmaningar från sina konkurrenter och hur de övervann dem, än om det skulle få liknande uppgifter från branschrapporter eller cybersäkerhetsenkäter.

EUROPEISKA UNIONENS
CYBERSÄKERHETSBYRÅ

OM ENISA

Europeiska unionens cybersäkerhetsbyrå, Enisa, är ett EU-organ som har till uppgift att säkerställa en hög nivå av cybersäkerhet i Europa. Europeiska unionens cybersäkerhetsbyrå, som grundades 2004 och stärktes genom EU:s cybersäkerhetsakt, bidrar till EU:s cyberpolitik och förbättrar tillförlitligheten hos produkter, tjänster och processer inom IKT genom program för cybersäkerhetscertifiering. Dessutom samarbetar byrån med medlemsstater och andra EU-organ, och hjälper Europa att förbereda sig inför morgondagens cyberutmaningar. Genom kunskapsspridning, kapacitetsuppbyggnad och åtgärder för att öka medvetenheten arbetar byrån tillsammans med sina huvudintressenter för att uppnå ökad tillit i den uppkopplade ekonomin, stärka motståndskraften i unionens infrastruktur och slutligen upprätthålla digital säkerhet för Europas samhälle och allmänhet. För mer information, besök www.enisa.europa.eu.

Enisa
Europeiska unionens cybersäkerhetsbyrå

Aten-kontoret
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki,
Grekland

Heraklion-kontoret
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Grekland

enisa.europa.eu